IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

DOMINIQUE CAVALIER AND
JUSTIN CAFFIER, individually and
on behalf of all others similarly situated,

Plaintiffs,

vs. Case No.:

NATIONAL DEBT RELIEF, LLC,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR TRIAL BY JURY

Plaintiffs Dominique Cavalier and Justin Caffier ("Plaintiffs"), on behalf of themselves and all others similarly situated, bring this action against National Debt Relief, LLC ("National Debt Relief," "NDR" or "Defendant") for its violations of their privacy by aiding, agreeing with, employing, or conspiring with various third parties to learn, use, or attempt to learn or use their sensitive, personal financial communications. Defendant's willful and affirmative actions aided numerous third parties to learn the contents of Plaintiffs' communications—as well as the communications of the members of the proposed Class—with NDR, including Meta, Google, Microsoft, Twitter, Tiktok, The Trade Desk, and Claritas (together, the "Third Parties"). Plaintiffs allege the following based upon personal knowledge as to their own conduct, the investigation of their counsel, and on information and belief:

NATURE OF THE CASE

1. NDR provides consumer debt relief services. As part of its business, it operates a website located at https://www.nationaldebtrelief.com/ (the "Website") which offers information

about NDR's debt relief services and facilitates a process through which visitors may apply for such services.

2. The Website's debt relief application requests users to submit information to establish a relationship with the company—soliciting sensitive, personal financial information from such users, including their current debt amount and personal information about themselves, such as their full name, phone number, and email address. In fact, the application process can only be completed by submitting this sensitive personal financial information ("PFI").

3. However, when NDR collects such PFI communicated by users, the Website aids, employs, and/or conspires with the Third Parties to capture and analyze the PFI for the purposes of marketing and advertising. NDR's installation of the Third Party technologies aids them, permits them, and/or causes them to learn or attempt to learn the contents of such communications, without the users' consent, in violation of California law.

4. In addition, users who communicate with NDR via the Website are subject to having their internet-connected machines "trapped and traced" by the Third Parties' technology which qualify as pen registers because they collect the users' IP addresses.

5. Both NDR and the Third Parties obtain a pecuniary benefit from NDR's installation of such surveillance technologies: NDR through enhanced analytics and improved advertising capabilities, and the Third Parties by improving their advertising services, leading to increased revenue. NDR purposefully traded its users' sensitive, personal financial information in exchange for these benefits.

6. At no point does any user of the website provide consent for any third party to capture and analyze their communications with NDR – including their communications of PFI.

7. NDR installed tracking technology from each of the Third Parties within its Website which aids each and every one of them to monitor, capture, and analyze the sensitive data and communications users send to NDR.

8. The Third Parties use such information to build profiles of individuals and target them with advertising on behalf of the Third Parties' clients. As one of their clients, NDR benefits from such data driven advertising practices in two ways: (1) by enhancing the effectiveness of the ads NDR places on the Third Parties' advertising networks and/or (2) by assisting NDR to make the most of its online presence where such Third Parties provide information and analysis on how users interact with the Website.

9. NDR's employment of such technology is unlawful: NDR's online users did not consent to any third party obtaining and/or learning the contents of their communications with NDR. Furthermore, the Third-Parties use the information collected for their own individual pecuniary interests, and NDR is solely responsible for aiding, agreeing with, employing, and/or conspiring with the Third Parties' to permit and/or cause them to learn, use, or attempt to learn or use such online communications.

10. Defendant's conduct violates (1) Cal. Penal Code § 631(a) and (2) Cal. Penal Code § 638.51.

11. Plaintiffs bring this action on behalf of themselves, and all others similarly situated to hold NDR accountable for its unlawful actions in aiding, agreeing with, employing, or conspiring with the Third Parties to learn and use the contents of its users' communications with the Website for any purpose.

THE PARTIES

12. Plaintiff, Dominique Cavalier ("Plaintiff Cavalier"), is a resident of Ontario, California. Within the last twelve months Plaintiff Cavalier applied for debt consolidation on NDR's Website.

13. Plaintiff, Justin Caffier ("Plaintiff Caffier"), is a resident of Los Angeles, California. Within the last twelve months, Plaintiff Caffier applied for debt consolidation on NDR's Website.

14. Defendant National Debt Relief, LLC is a New York corporation with its principal place of business at 180 Maiden Lane, 28th Floor, New York, NY 10038. National Debt Relief is a major debt relief company in the United States and operates the Website at https://www.nationaldebtrelief.com/.

JURISDICTION AND VENUE

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District.

16. The Court has general personal jurisdiction over Defendant because Defendant resides in and does business in the State of New York, with its principal place of business in New York, New York.

17. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. §§ 1332(a), 1332(d)(2) because this case is a class action where the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the proposed Class, and at least one class member is a citizen of a state different than Defendant.

LAWS AT ISSUE

A. CIPA

18. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638 ("CIPA") and was enacted to protect the privacy of Californians: "The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." CIPA § 630.

19. Cal. Penal Code § 631(a) provides that:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

Cal. Penal Code § 631 (West).

20. CIPA prohibits aiding or permitting another person to willfully and without the consent of all parties to a communication read or learn the contents or meaning of any message, report, or communication. CIPA applies to communications transmitted via computers, the

internet and email while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

21. Under Cal. Penal Code § 637.2, Plaintiffs and Class Members may seek injunctive relief and statutory damages of $5,000 per violation.

B. California Trap and Trace Law

22. California Penal Code Section 638.51 provides that "a person may not install or use a pen register or a trap and trace device without first obtaining a court order."

23. The law broadly defines a "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

24. A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

25. For example, in the context of email correspondence in which a person sends an email, a "pen register" records the email address from which an email was sent, the address receiving the email, and the subject line—because this constitutes the individual's outgoing information. On the other hand, if that same individual receives an email, a "trap and trace device" records the same information, but the record is reflected as incoming information.

26. The same kind of technology can be used to record an individual's IP address information, which is transmitted to the Third Parties when the user's browser submits its request

to load the website and at that time the Third Parties, via their technology, record the addressing information from the user. An IP address identifies the location of an internet-connected device and qualifies as dialing, routing, addressing, or signaling information.

27. Individuals may bring an action against the violator of any provision of CIPA—including CIPA § 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

FACTUAL ALLEGATIONS

A. The National Debt Relief Website

28. Defendant's Website offers visitors the ability to research and apply for debt consolidation and to learn about National Debt Relief and the services it offers. Upon accessing the Website domain at https://www.nationaldebtrelief.com/, users are brought to the home page shown below:

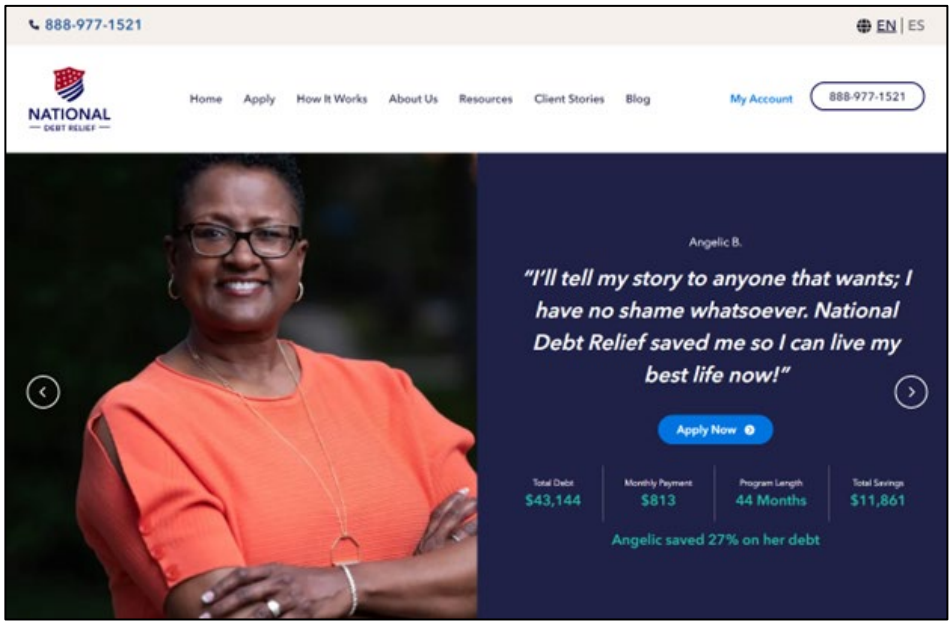

Figure 1

29. The "Apply Now" button on the NDR homepage (*see* Figure 1) opens the application process; on this page NDR requests the user to enter the amount of his debt.

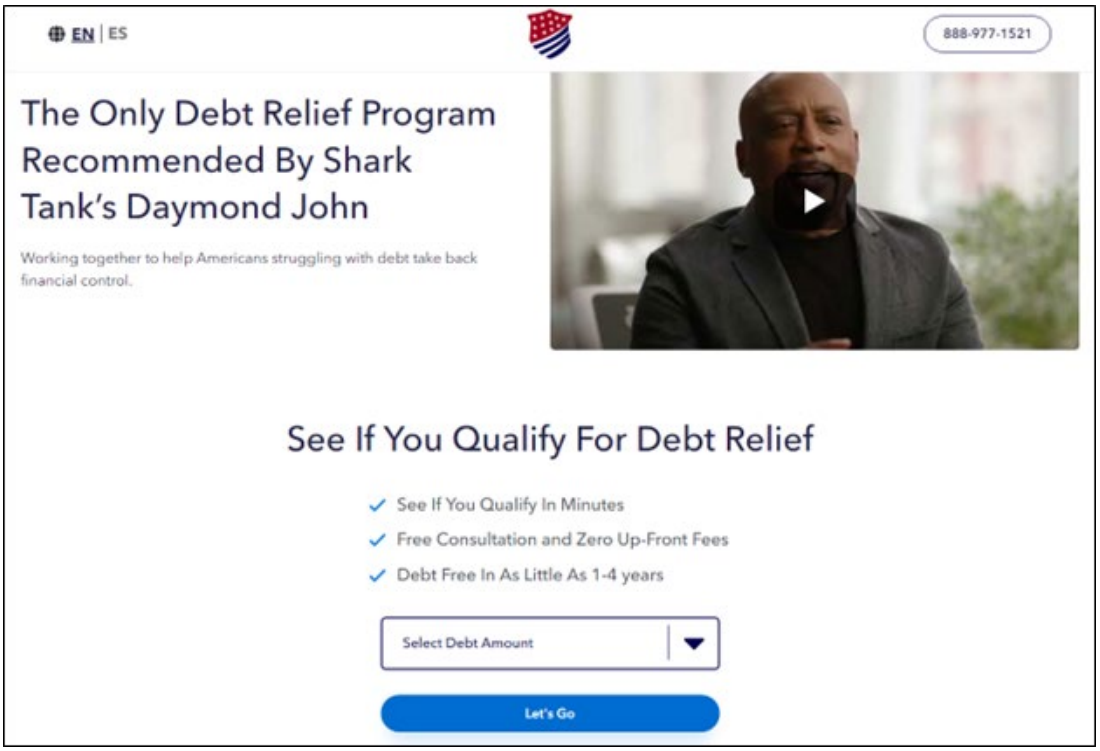

Figure 2

Figure 3

30. After informing NDR of the debt amount, a user who clicks the "Let's Go" button is presented with a form that requests him to submit his first name, last name, phone number, and

email address to continue with the application process. In fact, if the user wants to continue with the application, providing this information is mandatory.

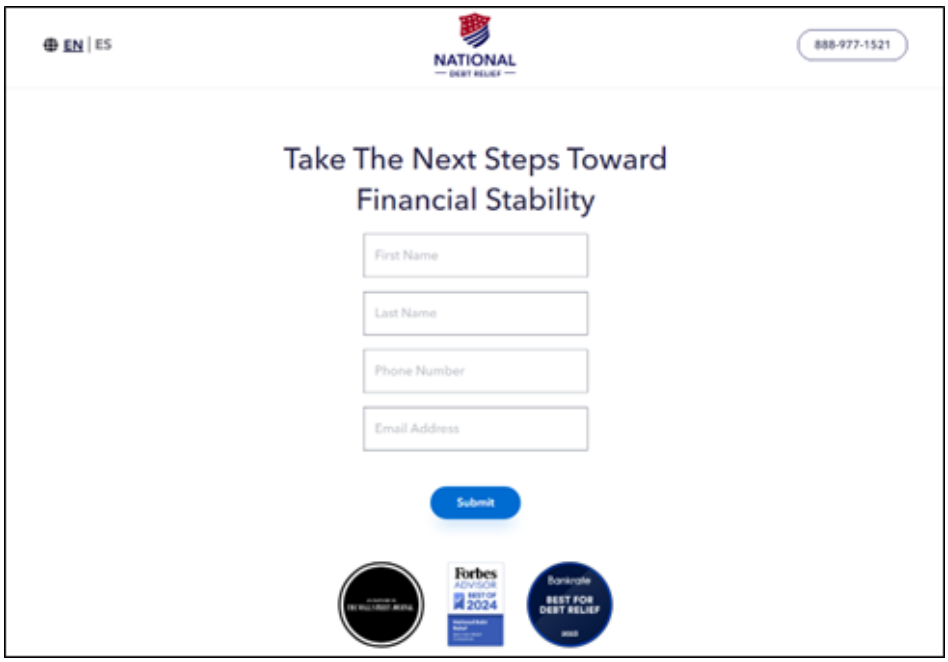

Figure 4

31. Next, NDR requires the user to enter his address and date of birth.

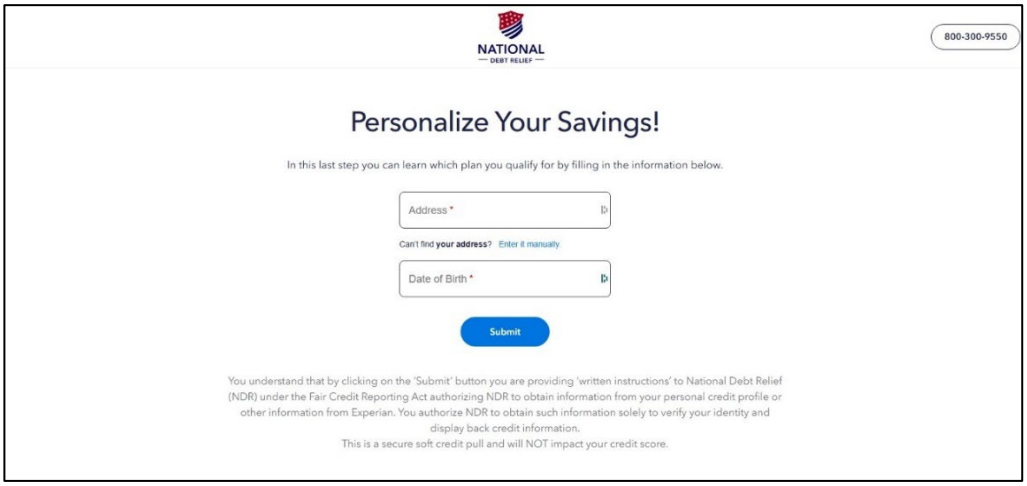

Figure 5

32. The Website then facilitates the applicant to add a family member to his plan by entering the family member's first and last name as well as his or her date of birth.

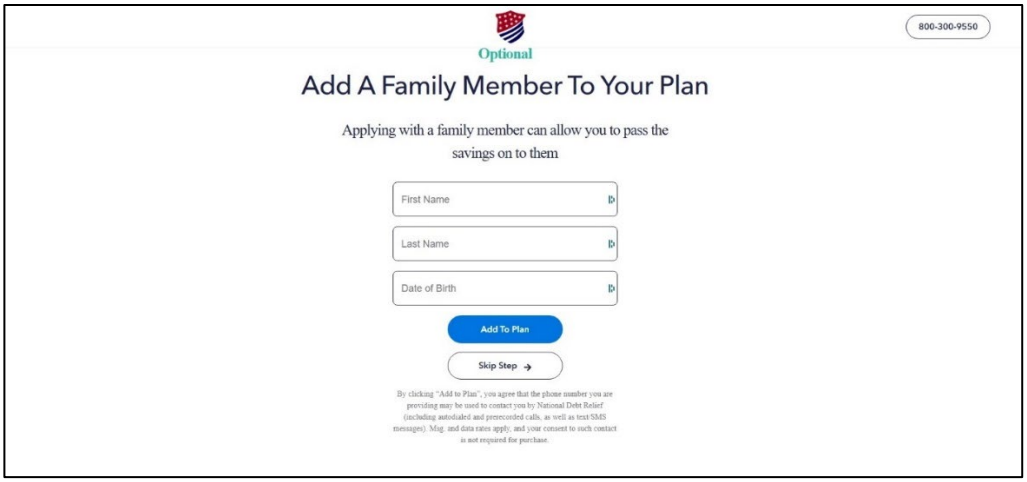

Figure 6

33. Finally, the applicant is required to provide his social security number to NDR, as well as the social security number of any added family members.

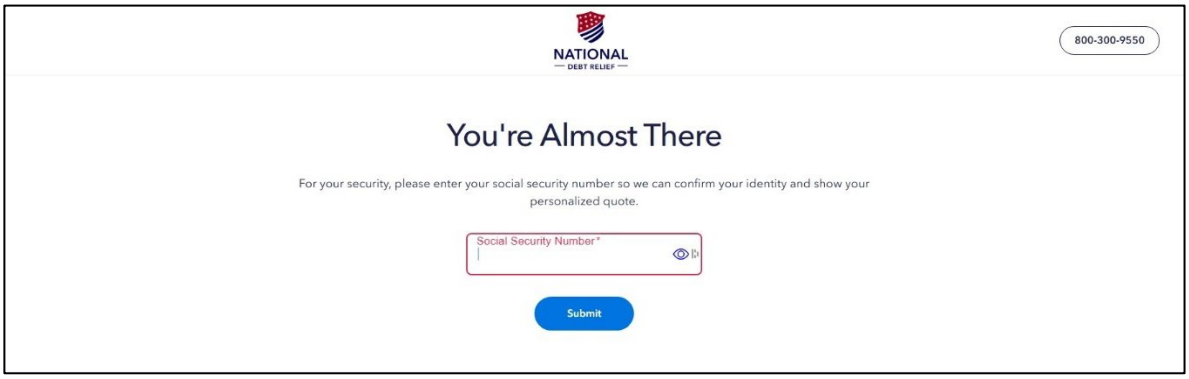

Figure 7

34. After completing the application process, NDR informs the applicant it will call him to continue the process.

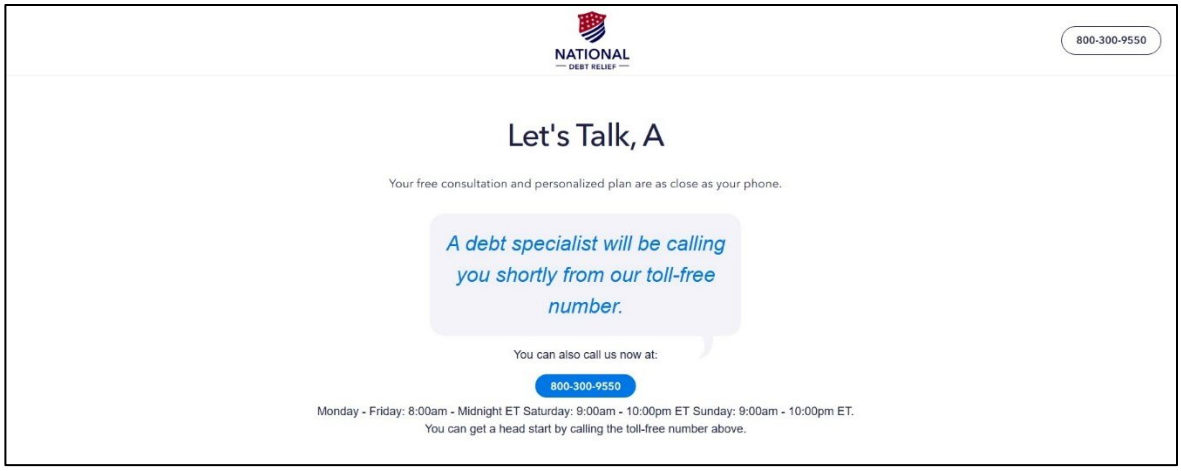

Figure 8

35. NDR configured its Website with surveillance technology designed by the Third Parties, which collects information online users and applicants provide to NDR, including their sensitive PFI and their communications with NDR.

36. The Third Parties' interception of users' communications and PFI, as aided by Defendant, includes the information they provide about their debt amount and their personal information (including contact information): all submitted by users to NDR to obtain information about and/or apply for its debt consolidation services. In addition to learning the contents of users' communications with NDR through its Website, the Third Parties collect unique user identifiers, which make them capable of using the information collected to re-direct and retarget advertising to those same users.

37. As used in this Complaint, unique identifiers are pieces of data that allow the Third Parties (and NDR) to recognize the user accessing the Website and facilitate their ability to send communications and information to the user at a later time. The unique identifiers used in this Complaint include but are not limited to:

a. Names;

b. Email addresses;

c. Home and mailing addresses;

d. Phone numbers;

e. Internet Protocol (IP) addresses;

f. Device identifiers; and

g. Cookies, which are unique pieces of code that websites install within a user's browser, and which allow technology familiar with the cookie and the particular user's cookie's values to recognize that same user when they re-visit the Website or visit other websites on which such technology is installed.

38. As discussed further below, NDR's facilitation of the Third Parties interception of PFI violates sections 631 and 638 of CIPA.

B. Third Party Tracking Companies

i. Meta's Platform and Tracking Technology.

39. **The Meta Platform.** Meta Platforms, Inc. ("Meta") is an advertising company. It sells advertising space on the social media and technology platforms it operates, including on Facebook. Meta's advertising services are top-of-the-line due to its sophisticated data-collection tools which collect voluminous information about how millions of unique individuals interact with webpages both on its platforms and across the internet. After gathering such information, Meta employs innovative user categorizing systems to understand and predict how such individuals will engage with content in the future. These systems then retarget the individuals with advertisements from Meta's clients - advertisements which are more effective due to Meta's pervasive surveillance of internet users.

40. Its expansive tracking enables Meta to make highly personal inferences about users, such as about their "interests" and "behavior."[1] Meta compiles information it obtains and infers about internet users and uses it to identify personalized "audiences" to target users likely to respond to particular advertisers' messaging. Access to such audiences is extremely valuable to Meta's advertising clients. In the twelve months ending September 30, 2024, Meta has generated over $150 billion.[2]

41. **The Meta Pixel**. The Meta Pixel (" Meta Pixel") is a string of code that a website owner can install within its website, and which operates to improve the effectiveness of the website's digital advertising by helping Meta better understand the website owner's audience. The Meta Pixel monitors the website's users as they interact with the website and because it is installed on thousands of other webpages, Meta also learns what those same users do on *other* websites. The Meta Pixel is a primary means through which Meta acquires personal information about users to create customized audiences for its advertising business. The Meta Pixel transmits to Meta immense information about each user's interactions with each website where it is embedded.

42. A business which purchases advertising space on Meta's platform, such as NDR, is encouraged to install a Meta Pixel because it facilitates Meta's surveillance of users' communications, activities, and interactions. This, in turn, allows Meta to deliver advertising to an audience of individuals most likely to respond to it (i.e., by clicking on it and hopefully making a purchase).

---

[1] Meta, *Ad Targeting: Help your ads find the people who will love your business*, https://www.facebook.com/business/ads/ad-targeting.

[2] Meta Platforms Revenue 2010-2024, https://www.macrotrends.net/stocks/charts/META/meta-platforms/revenue#:~:text=Meta%20Platforms%20revenue%20for%20the,increase%20year%2Dover%2Dyear (last visited December 2, 2024).

43. The Meta Pixel operates automatically when the user loads the website to monitor, record, collect, and analyze all of the users online interactions. For every communication that occurs between a user and a website outfitted with a Meta Pixel (including NDR's Website), the Meta Pixel aids Meta in receiving a copy of such communication for use and analysis.

44. NDR does not obtain consent from users to facilitate Meta's surveillance of the user's interactions with NDR's Website.

45. As depicted in the forensic analysis below, the Meta Pixel aids Meta in learning or attempting to learn information about users' activities NDR's Website. Specifically, when a user proceeds through NDR's application process Meta learns the user's name, phone number, email address, that the user is applying for NDR's debt consolidating services, and the amount of debt the user has.[3]

[3] Allen Carney is an attorney with Carney Bates & Pulliam, PLLC. Forensic analysis used in this complaint was conducted under his identity on the NDR website for case investigation purposes. The network traffic generated by those interactions with NDR's website are representative of and substantially similar to network traffic generated by any user visiting NDR's website.
The left half of Figure 9 illustrates the web proper being analyzed, and the right half depicts the network traffic transmitting information from the user's browser with the host website and any other Third Parties whose technology is installed on the webpage, such as Meta's Pixel. Figure 10 highlights portions of such network traffic from Figure 9.

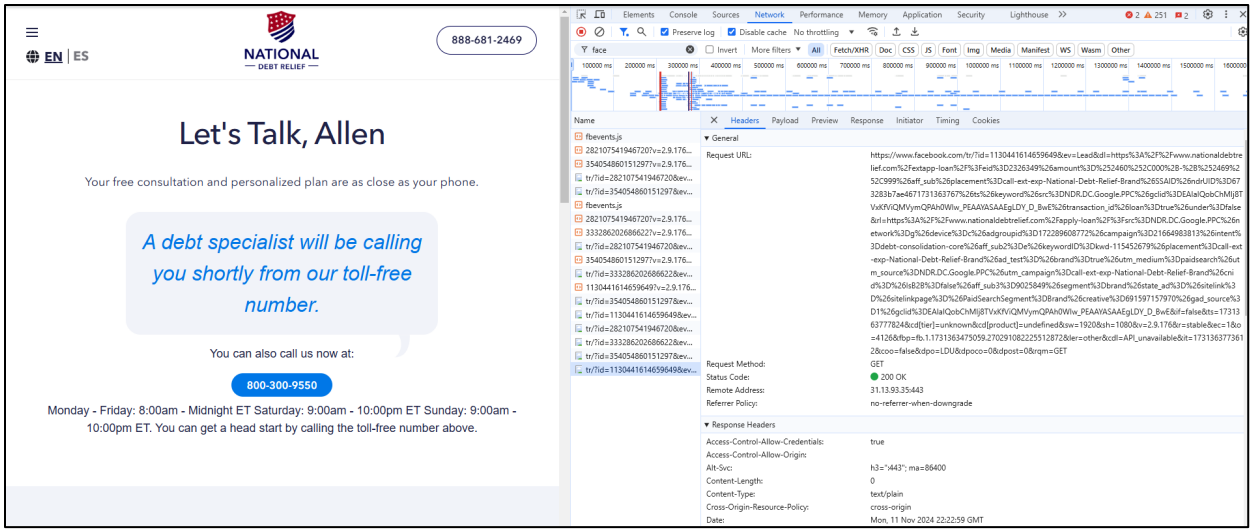

Figure 9

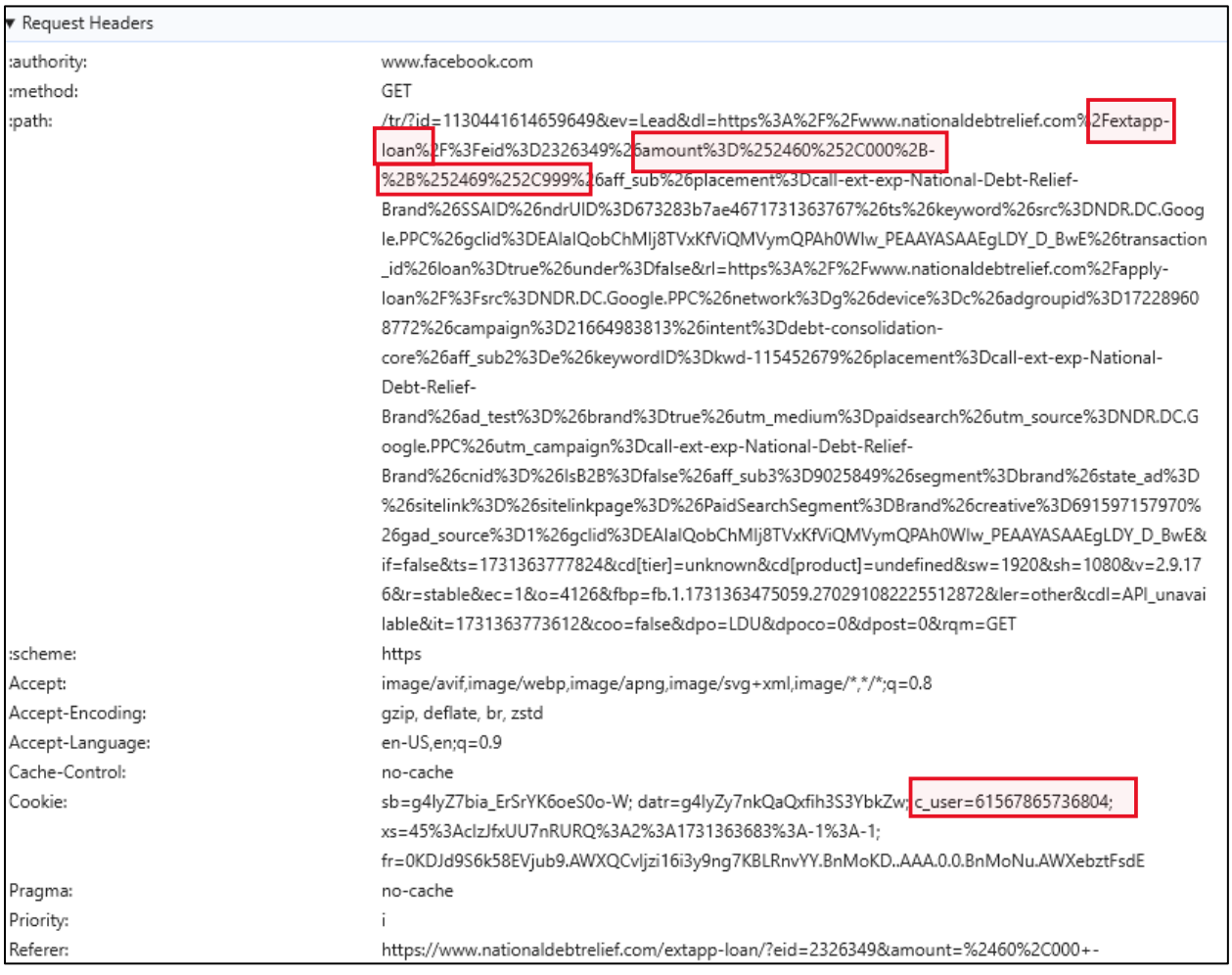

Figure 10

46. When Meta intercepts such user communications to NDR, the Pixel transmits unique identifiers to Meta which identify the user, including but not limited to his or her Facebook ID, and indicate the user is a person interested in debt relief services. This makes Meta capable of serving the user with advertising relevant to debt relief services.

47. In sum: the Pixel collects user's interactions and communications with various websites, like NDR's, and transmits them to Meta so that Meta can target advertising back to users, benefiting both Meta and the websites which host a Pixel.

ii. Google's Platform and Tracking Technology.

48. **Google**. Google is the world's largest advertising platform offering multiple products with billions of users worldwide.[4]

49. According to Google, "[a]dvertising is what makes it possible to offer [Google's] products to everyone…[Google] make[s] the vast majority of [its] money from advertising."[5] Recently, in 2023, Google was estimated to generate "roughly 38 percent of the global [digital] ad revenue."[6] Like Meta, Google engages in widespread and sophisticated targeted advertising through its advertising product "DoubleClick."[7]

50. Through its operation of DoubleClick, Google can make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more.[8] The personal information and communications obtained by Google through

[4] Statista Research Department, *Share of major ad-selling companies in digital advertising revenue in the United States from 2021 to 2026*, Jun. 25, 2024, https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/.
[5] About Google, *How our business works*, https://about.google/how-our-business-works/
[6] Statista Research Development, *Advertising revenue generated by Google from 2017 to 2027*, STATISTA.COM (Aug. 25, 2023), https://www.statista.com/statistics/539447/google-global-netadvertising-revenues/.
[7] Google, *Targeting your ads*, GOOGLE.COM, https://support.google.com/googleads/answer/1704368?hl=en (last visited December 2, 2024).
[8] Google, *About audience segments*, GOOGLE.COM, https://support.google.com/googleads/answer/2497941?hl=en&ref_topic=10545551&sjid=10176374672745389741-NC (last visited December 2, 2024).

DoubleClick are funneled into its marketing and advertising businesses and are used to fuel various services offered via Google's Marketing Platform to allow advertisers to reach new customers.[9]

51. Like Meta, Google's user-tracking and targeted advertising services rely on its ability to obtain communications and user-interactions from any website on which its technology is installed – like NDR's. The personal information obtained and learned by Google is extremely valuable to Google and its marketing and advertising clients because the inferences derived from users' personal information allow marketers and advertisers to target potential customers.

52. In 2022, "Google generated 224.5 billion U.S. dollars in advertising revenue."[10] That figure is expected to reach "nearly 340 billion U.S. dollars by 2027."[11]

53. **Google DoubleClick**. Google "DoubleClick" is a tracking tool installed by website owners which transmits information about their users and their users' online interactions to Google. Although not required for any website to function, Website owners may install the DoubleClick code on their websites to capture and transmit records of user interactions and communications to Google through HTTP requests. Google then processes the data and adds it to categorized datasets, forming the basis for the targeted advertising that Google sells to its marketing and advertising customers.

54. If a user visits a website embedded with Doubleclick, Google receives HTTP requests similar to those sent to Meta recording the user's interactions and including identifying information about the unique user stored in cookies on the user's browser.

---

[9] *See Google, Case Study McDonald's Hong Kong uses Google Analytics 4 to increase in-app orders by 550%,* GOOGLE.COM, https://marketingplatform.google.com/about/resources/mcdonald-hong-kong-uses-google-analytics-4-to-increase-in-app-orders-by-550-percent/ (last visited December 2, 2024).
[10] Statista Research Development, *supra* note 6.
[11] *Id*.

55. For example, via DoubleClick, Google learns Allen Carney's full name, email address, phone number, amount of his current debt, and that he is filling out an application for debt consolidation with NDR.

Figure 11

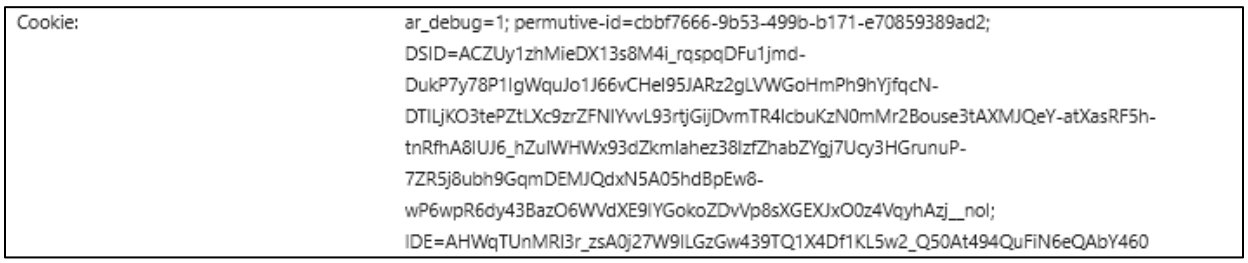

Figure 12

56. With this information in hand, DoubleClick constructs user profiles using data compiled through cookies and tracking technologies. These profiles include the personal information users submit (like email addresses and debt amount) and are employed to tailor advertising to users' preferences, updating users' profiles based on their current online behavior.

57. Google then uses the compiled user information to sell specific tools to its customers to provide even greater enhancements to their advertising spend. Google markets and sells to its customers the ability to target Affinity Audiences, Custom Affinity Audiences, and In-Market Audiences based on users' interest in products, services, or pastimes related to the advertisers' business.[12]

58. **Google Analytics**. Google Analytics is a Google marketing product, used for advertising and analytics to enhance the effectiveness of online advertising. A fundamental purpose of Google Analytics is to collect information about online users' communications and interactions with the web properties of non-Google entities. To obtain the benefits of this product, a website owner (such as NDR) must configure and install Google Analytics tracking code within its website code.

59. NDR configured the Google Analytics code on the Website to transmit users' amounts of debt, full names, email addresses, phone numbers, and IP addresses to Google.

60. To make NDR's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to NDR's server where the relevant Website data is stored. In response to the request, NDR's server sends an "HTTP response" back to the browser with a set of instructions.

[12] Google Ads Help, *About audience segments*, GOOGLE https://support.google.com/google-ads/answer/2497941?hl=en (last visited December 2, 2024).

61. In addition to transmitting a user's communications to Google, its code causes the browser to send the user's IP address to Google through HTTP requests simultaneous with the user's communications with NDR and interactions on its Website. Google then records this IP address which it further uses to collect information about the user.

62. The IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (e.g., 192.168.123.132). The first two sets of numbers indicate what network the device is on (e.g., 192.168), and the second two sets of numbers identify the specific device (e.g., 123.132).

63. Thus, the IP address enables a device to communicate with another device—such as a computer's browser communicating with a server—and the IP address contains geographical location.

64. IP addresses can be used to identify the device's state, city, and zip code.

iii. X Corp.

65. **The X Corp. Platform.** X Corp. ("X") sells advertising space on the social media platform it operates.[13] Like Meta and Google, X's advertising is based on sophisticated categorizing and targeting capabilities fueled by the personal data of users of the social media platform and other internet users.[14] X's targeting abilities are exceptional, because X surveils users' online activities both on and off X's own platform.[15] This expansive tracking enables X to

[13] *Advertising*, X CORP., https://business.x.com/en/advertising.html (last visited Aug. 26, 2024).
[14] *X Ads Targeting*, X CORP., https://business.x.com/en/advertising/targeting.html (last visited Aug. 26, 2024).
[15] Tim Starks, *A Twitter Data Tracker Inhabits Tens of Thousands of Websites*, WASH. POST (Dec. 8, 2022, 7:21 AM), https://www.washingtonpost.com/politics/2022/12/08/twitter-data-tracker-inhabits-tens-thousands-websites/; *Which Websites Are Sharing Data About Consumers with Elon Musk's Twitter?*, ADALYTICS, https://adalytics.io/blog/websites-sharing-data-with-Twitter (last visited Aug. 26, 2024); *Optimized Targeting*, X CORP., https://business.x.com/en/help/campaign-setup/campaign-targeting/optimized-targeting.html (last visited Aug. 26, 2024).

make highly personal inferences about users, including their interests, behavior, and connections.[16]

66. X compiles information it obtains about internet users and uses it to infer information about them and to identify personalized custom "audiences" likely to respond to particular advertisers' messaging.[17] Access to such audiences is extremely valuable to X's advertising clients. In the first six months of 2022, X generated approximately $2.2 billion, nearly 92% of its revenue for the period, through advertising.[18]

67. **The X Corp. Tracking Pixel.** The X Corp. Tracking Pixel ("X Pixel") is a primary means through which X acquires personal information to create custom audiences for its advertising business.

68. NDR employs the X Pixel alongside X's Universal Conversion Tracking Tag (uwt.js), which is a JavaScript file that collects various meta-data about a user's browser, device, and IP address.[19]

69. X encourages the use of a subdomain alongside the X Pixel: analytics.twitter.com which facilitates the transmission of an X user's twid, among other personal information.[20]

70. The twid is a unique identifier associated with every X user's profile when the profile is created. Because it is consistent and unique to each X user, X uses it to uniquely identify

---

[16] *How X Ads Work*, X CORP., https://business.x.com/en/help/troubleshooting/how-x-ads-work.html (last visited Aug. 26, 2024).
[17] *X Ads Targeting*, X CORP., https://business.x.com/en/advertising/targeting.html (last visited Aug. 26, 2024).
[18] SECURITIES AND EXCHANGE COMMISSION, *Twitter, Inc. Form 10-Q* 13 (filed July 27, 2022), https://www.sec.gov/Archives/edgar/data/1418091/000141809122000147/twtr-20220630.htm#ia3cbe6e67be64784a54868590f38351c_19 (showing advertising services made up $2.18B of the total $2.38B of recognized revenue).
[19] Adalytics, *supra* note 4; *Conversion API Set Up*, X Corp., https://developer.x.com/en/docs/x-ads-api/measurement/web-conversions/conversion-api (last visited Aug. 26, 2024).
[20] *Conversion Tracking for Websites*, Twitter (Nov. 22, 2022) https://web.archive.org/web/20221122201058/https://business.twitter.com/en/help/campaign-measurement-and-analytics/conversion-tracking-for-websites.html; *Conversion Tracking for Websites*, X Corp., https://business.x.com/en/help/campaign-measurement-and-analytics/conversion-tracking-for-websites.html (last visited Aug. 26, 2024).

them. Due to NDR's integration of the X Pixel, X can identify specific individuals that communicate with NDR via its Website as well as the contents of such communications.

71. X learns users' full names, emails, phone numbers, current amounts of debt, and that they are applying for debt consolidation with NDR via the Website.

iv. Microsoft, TikTok, The Trade Desk, and Claritas

72. **Microsoft**. Microsoft's Universal Event Tracking Tag ("UET Tag") "records what customers do on your website and sends that information to Microsoft Advertising."[21] The UET Tag "enables or enhances many key Microsoft Advertising features [including] Conversion tracking [and] Audience targeting."[22]

73. The UET Tag uses the "MUID" cookie, which "contains a [globally unique identifier] assigned to your browser. It gets set when you interact with… a UET beacon call through the browser."[23] In general, the MUID cookie and IP address are transmitted with http requests via UET Tag.[24]

74. Like Meta's, Google's, and X's online tracking technologies, Microsoft's UET Tag relies on unique identifies stored within cookies to uniquely identify online individuals and allows Microsoft to obtain records of exactly what communications users send to websites that implement its technology, including NDR.

75. In addition to transmitting a user's communications to Microsoft, its code causes the browser to send the user's IP address to Microsoft through HTTP requests simultaneous with

[21] Microsoft Advertising, *What is UET and how can it help me?*, Microsoft https://help.ads.microsoft.com/#apex/ads/en/56681/2 (last visited December 2, 2024).
[22] *Id.*
[23] Microsoft, *FAQ: Universal Event Tracking*, Microsoft https://help.ads.microsoft.com/#apex/ads/en/53056/2 (last visited December 2, 2024).
[24] *Id.*

the user's communications with NDR and interactions on its Website. Microsoft then records this IP address which it further uses to collect information about the user.

76. **TikTok**. TikTok Pixel is "a piece of code that you can place on your website that allows you to share website events with TikTok… The pixel collects information available via standard web browsers, like Chrome. This includes… IP Address: Used to determine the geographic location of an event…[and] Cookies: Used to help with the measurement, optimization, and targeting of your campaigns… third-party cookies are on by default with the TikTok Pixel."[25]

77. NDR configured its TikTok Pixel to utilize TikTok's "AutoAdvanced Matching Technology" which scans information from *every* website to determine identifying information associated with website visitors – whether TikTok users or not. The information this service obtains extends to name, date of birth, and address, which allows TikTok to determine with a great deal of accuracy which individuals it will target with advertisements.

[25] TikTok: Business Help Center, *About TikTok Pixel*, TikTok https://ads.tiktok.com/help/article/tiktok-pixel (last visited December 2, 2024).

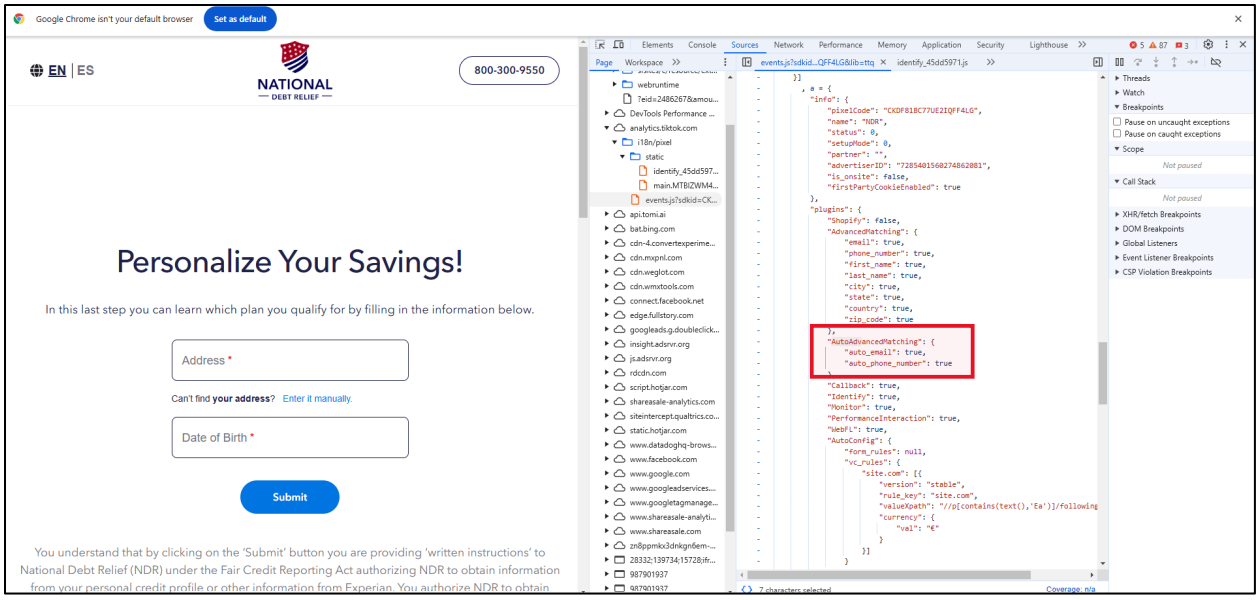

Figure 13

78. The TikTok Pixel utilizes the "_ttp" cookie, an advertising cookie containing a unique identifier used to match a user to their activities on the website which the TikTok Pixel is installed.[26]

79. NDR configured and installed the TikTok Pixel on the Website to send back to TikTok the _ttp cookie in conjunction with communications users submit when applying for debt relief services on the Website.

80. TikTok uses the information transmitted via the TikTok Pixel NDR installed on the Website to "deliver advertising, including targeted advertising, to [users of those websites] on

[26] TikTok: Business Help Center, *Using Cookies with TikTok Pixel*, TikTok https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?redirected=1 (last visited December 2, 2024); TikTok for Business Developers, *Set up TikTok Click ID and Cookies*, TikTok https://business-api.tiktok.com/portal/docs?id=1739584860883969 (last visited December 2, 2024).

[TikTok]."[27] Tiktok also shares this information with its business partners for, among other things, "search engine optimization, data processing" and "advertising and marketing services."[28]

81. Like Meta's, Google's, and X's online tracking technologies, TikTok's technology relies on unique identifiers, such as the TikTok User ID, stored within cookies to uniquely identify online individuals and allow TikTok to learn the communications users send to websites that install its technology, including NDR.

82. **The Trade Desk**. The Trade Desk Universal Pixel ("TD Pixel") is a piece of JavaScript code, "that is placed on a webpage to track visitor activity on the page for the reporting and attribution purposes… tracking tags can pass information about pages visited or user actions taken on a given page, such as pressing buttons or making selections."[29]

83. Here, NDR integrated the TD Pixel into its Website, configuring the information it would intercept and transmit to The Trade Desk. Thus, when the TD Pixel fires on the Website, it transmits users' amount of debt, full names, phone numbers, email addresses and that the user is filling out an application for debt consolidation on the Website.

84. In addition to contents of users' communications with NDR, The Trade Desk receives a "TDID cookie" – a unique identifier assigned to each person who uses a website where the TD Pixel is installed.

85. The Trade Desk further permits a website to directly monetize the data it allows the TD Pixel to extract: on information and belief, The Trade Desk sells data it intercepts from the Website to its advertising clients for targeted advertising campaigns.[30]

---

[27] TikTok, *Privacy Policy*, TikTok https://www.tiktok.com/legal/page/us/privacy-policy/en (last visited December 2, 2024).
[28] *Id.*
[29] The Trade Desk, *Tracking Tags*, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsOverview (last accessed Nov. 14, 2024).
[30] The Trade Desk, *Getting Started for Merchants*, https://partner.thetradedesk.com/v3/portal/data/doc/DataGetStartedMerchant (last visited Nov. 14, 2024).

86. **Claritas**. Claritas is a "data-driven marketing company" that uses unique data and its proprietary "identity graph," to help businesses identify users, gather data on them, and target advertising to them.[31]

87. Claritas promotes itself as having "transformative technology and superior data science to connect your customers' and prospects' real-world data to their devices and digital behavior with more accuracy and scale than anyone in the industry… The Claritas Identity Graph reaches nearly 100% of US consumer households and ties together over 40 billion data points monthly to produce the highest-def portrait of each customer and prospect."[32]

88. Claritas builds this vast dataset, in part, through its AudienceAnywhere Pixel (the "Claritas Pixel") which it offers to its business customers as part of its services.[33]

89. The Claritas Pixel is a block of JavaScript code advertisers configure and install on their websites in order to transmit back to Claritas users' actions and activities on the websites.[34]

90. NDR configured and installed the Claritas Pixel on the Website. NDR configured it to transmit users' debt amounts, full names, email addresses, and phone numbers back to Claritas to use for its own independent advertising purposes.

91. Within the Claritas Pixel on NDR's Website is the barometric[cuid] cookie which contains an anonymous identifier (CUID) associated with the user.[35] Claritas uses the

[31] Claritas, *Turning Data into Growth: Meet Claritas*, Claritas https://claritas.com/about/ (last visited December 2, 2024).
[32] Claritas, *Claritas Identity Graph*, Claritas https://claritas.com/claritas-identity-graph/ (last visited December 2, 2024).
[33] Claritas, *Privacy & Legal*, Claritas https://claritas.com/privacy-legal/ (last visited December 2, 2024).
[34] Claritas, *AudienceAnywhere Tag Implementation Guide*, Claritas https://claritas360.claritas.com/knowledgecenter/help/content/audienceanywhere/documents/audienceanywhere%20-%20tag%20implementation%20guide.pdf (last visited December 2, 2024).
[35] LinkedIn, *LinkedIn Cookie Table*, LinkedIn https://www.linkedin.com/legal/l/cookie-table (last visited December 2, 2024); PennState Health, *Cookie Declaration*, Penn State Health https://www.pennstatehealth.org/cookie-declaration (last visited December 2, 2024).

barometric[cuid] cookie to group users into segments in order to serve them with targeted advertising.[36]

92. Moreover, Claritas touts that "[e]very visitor to a website leaves behind a digital trail that includes an anonymous identifier. By placing a pixel on your website, Claritas captures that website user information. Then using our industry-leading Identity Graph, we combine this website data with your… data… to create a more complete profile of the anonymous visitor. The Claritas Identity Graph helps you know even more by filling in information about each potential buyer, including household information and demographic data, along with information on the ideal channels you should use to reach him or her."[37]

93. By configuring and installing the Claritas Pixel on its Website, NDR aids Claritas in its interception, compilation, and use of the sensitive information transmitted for its own benefit and the benefit of any of its business customers.

94. In addition to transmitting a user's communications to Claritas, its code causes the browser to send the user's IP address to Claritas through HTTP requests simultaneous with the user's communications with NDR and interactions on its Website. Claritas then records this IP address which it further uses to collect information about the user.

C. NDR Aids the Third Parties To Learn, Use, or Attempt To Learn Or Use Its Users' Communications And Their PFI.

95. The Third Parties' technology is not necessary for the Website's functions.

[36] Claritas, *Claritas Identity Graph*, Claritas https://claritas.com/claritas-identity-graph/ (last visited December 2, 2024).
[37] Claritas, *Identifying Anonymous Website Visitors*, Claritas https://claritas.com/anonymous-website-visitors/ (last visited December 2, 2024).

96. The Third Parties' technologies do not simply appear on a website by happenstance; indeed, a website owner must obtain the necessary code and implement such surveillance technology on its website. This is precisely what NDR did here.

97. NDR agreed to use, configured, employed, and maintains the Third-Party technology on its Website, aiding the Third Parties to learn, use, and attempt to learn or use Website users' online communications and their PFI. In return, the Third Parties provide NDR with benefits associated with their online web presence. NDR's aiding the Third Parties' interception of users' PFI was and is deliberate.

98. NDR specified the types of information it desired the Third Parties to extract from its Website, such as its user's communications with it—including communications regarding their amount of debt and their applications for debt consolidation.

99. On the Website, the Third Parties' technologies are active on each page users can visit.

100. When NDR's users apply for debt relief using the Website, they communicate their personal information to NDR with the goal of receiving a response from NDR regarding its ability to provide such debt relief and simultaneously the Third Parties' technology surreptitiously intercepts Class members' communications by transmitting records and contents of their interactions as they submit them to the Website.

101. NDR did not obtain consent to deploy such technology.

D. Communications Related to Financial Information are Sensitive and Should be Kept Confidential.

102. NDR's aiding the Third Parties in their attempts to learn or use the contents of its user's communications violate established industry standards.

103. For example, in testimony before the House Financial Services Committee Task Force on Financial Technology, on November 21, 2019, a representative for the American Bankers Association explained that the association had "developed a set of principles – consistent with the CFPB and the rest of industry," to help protect consumers in the context of financial data aggregation. Those principles include:

> **Transparency** – Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data a technology company are accessing, how long the company is holding this data, and how it is using the data.
>
> **Control** – When consumers share their financial data, they should have control over what information is shared and how it is used. Intuitive control would allow consumers to see easily who is authorized to receive their data, modify what access they have, and revoke that access when a service is no longer used.
>
> **Minimization** – Consumers should expect that data-sharing is limited to the data that are needed to provide the service they have authorized and only maintain these data as long as necessary.[38]

104. The World Economic Forum has also identified guiding principles for the industry based upon multistakeholder workshops, meetings of senior industry and public-sector leaders, and expert interviews, which include similarly defined principles of "consent," and "control."[39] NDR's conduct conflicts with these widely recognized principles.

105. Despite these ubiquitous and universally appreciated privacy norms NDR shares its users' sensitive financial communications with a host of undisclosed Third Parties to obtain a better return on its marketing investments.

TOLLING

[38] *See* Nov. 21, 2019 Statement of American Bankers Association to House Financial Services Committee Task Force on Financial Technology, https://www.aba.com/advocacy/policy-analysis/data-access-statement-for-the-record.

[39] See World Economic Forum, The Appropriate Use of Customer Data in Financial Services (Jan. 20, 2020), http://www3.weforum.org/docs/WEF_FSIEG_Customer_Data_Preamble_And_Principles.pdf.

106. The statutes of limitation applicable to Plaintiffs' claims are tolled as a result of NDR's knowing and active concealment of its conduct alleged herein.

107. Through no fault or lack of diligence, Plaintiffs and members of the Class were deceived and could not reasonably have discovered Defendant's deception and unlawful conduct. The circumstances of NDR's conduct on and with respect to the Website would lead reasonable users to believe NDR was not facilitating the interception of their PFI.

108. Further, under the circumstances NDR was under a duty to disclose the true character, quality, and nature of its activities to Plaintiffs and obtain their consent. NDR therefore is estopped from relying on any statute of limitations.

109. All applicable statutes of limitations also have been tolled by operation of the discovery rule. Specifically, Plaintiffs and members of the Class could not have learned through the exercise of reasonable diligence of NDR's conduct as alleged herein.

PLAINTIFF SPECIFIC ALLEGATIONS

110. Plaintiff Cavalier is a resident of Ontario, California. Plaintiff Cavalier applied for debt consolidation on the NDR Website on or around January of 2024 at which time he sent communications to NDR including his current amount of debt, full name, email address, mailing address, and telephone number. NDR aided the Third Parties' interception of Plaintiff Cavalier's communications with NDR and their acquisition of his PFI without his consent.

111. Plaintiff Caffier is a resident of Los Angeles, California. Plaintiff Caffier applied for debt consolidation on the NDR Website on or around June of 2024 at which time he sent communications to NDR including his current amount of debt, full name, email address, mailing address, and telephone number. NDR aided the Third Parties' interception of Plaintiff Caffier's communications with the Website and their acquisition of his PFI without his consent.

CLASS ACTION ALLEGATIONS

112. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1 through 111 set forth above.

113. Plaintiffs bring this action as a class action pursuant to Rules 23(a) and (b) of the Federal Rules of Civil Procedure, on behalf of the following class: All individuals in California who submitted an application using the Website.

114. Excluded from the Class are Defendant, any controlled person of Defendant, as well as the officers and directors of Defendant and the immediate family members of any such person. Also excluded are any judge who may preside over this cause of action and the immediate family members of any such person. Plaintiffs reserve the right to modify, change, or expand the Class definition based upon discovery and further investigation.

115. **Numerosity—** The Class consists of at least hundreds of individuals, making joinder impractical.

116. **Commonality and Predominance—**Common questions of law and fact exist with regards to the claims and predominate over questions affecting only individual members of the Class. These common legal and factual questions include the following:

a. Whether Defendant aided, agreed with, employed, or conspired with the Third Parties to permit or cause the Third Parties to learn, or attempt to learn, the contents of Plaintiffs' and the Class members' communications with NDR;

b. Whether Defendant aided, agreed with, employed, or conspired with the Third Parties to permit or cause the Third Parties to use, or attempt to use,

the information it obtained from capturing Plaintiffs' and the Class members' communications with NDR;

c. Whether Defendant installed software which records or decodes dialing, routing, addressing, or signaling information in the form of IP addresses transmitted by Plaintiffs' and Class members' electronic devices which is likely to identify the source of their electronic communications;

d. Whether Defendant's aiding the Third Parties to learn its users' sensitive personal financial information, such as debt amount and contact information, constitutes learning the contents or meaning of users' messages or communications with NDR;

e. Whether Plaintiffs' and Class members' submission of information to Defendant's Website constitutes communications in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California;

f. Whether Defendant obtained consent to aid, agree with, employ, or conspire with the Third Parties to learn and/or use the contents of their communications with NDR;

g. Whether Defendant's conduct violates Cal. Penal Code § 631(a);

h. Whether Defendant's conduct violates Cal. Penal Code § 638.51.

117. **Typicality-** Plaintiffs' claims are typical of the claims of the Class and Plaintiffs have substantially the same interest in this matter as other members of the Class. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of the other members of the Class. Plaintiffs' claims arise out of the same set of facts and conduct as all other members of the

Class. Plaintiffs and all members of the Class who are users of the Website are victims of Defendant's unlawful Website design which procured the Third Parties to collect users' communications, including PFI for Defendant's and the Third Parties' financial gain. All claims of Plaintiffs and members of the Class are based on Defendant's wrongful conduct.

118. **Adequacy of Representation—**Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained competent counsel experienced in complex class action privacy litigation and Plaintiffs will prosecute this action vigorously. Plaintiffs have no interests adverse or antagonistic to those of the Class.

119. **Declaratory and Injunctive Relief** – Defendant acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making appropriate final injunctive relief and/or declaratory relief, as described below.

120. **Superiority—** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual members of the Class are small compared with the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the members of the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if the members of the Class could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and

comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

COUNT I
Violation of CIPA
Cal. Penal Code 631
(Against All Defendants)

121. Plaintiffs incorporate and reallege the above factual allegations paragraphs 1 through 120 as if fully alleged herein.

122. Plaintiffs bring this Count individually and on behalf of the members of the Class.

123. Cal. Penal Code § 631(a) provides that: "Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500)."

124. NDR aided, agreed with, employed, and/or conspired with the Third Parties to learn or attempt to learn the contents, of Plaintiffs' and the Class members' communications with NDR.

125. NDR also installed the technology across its Website so the Third Parties could use, attempt to use, or communicate the information so obtained, which NDR and the Third Parties did use and/or communicate for their own purposes.

126. NDR's installation of the technology on its Website permitted the Third Parties and caused them to learn and use, and to attempt to learn and to use, the contents of its users' communications with NDR.

127. NDR's aiding, employing, or conspiring with the Third Parties to collect, learn, and/or use the information they unlawfully obtained was willful.

128. Plaintiffs and Class members transmitted such communications to NDR using wires, lines, or cables within California, sent their communications from California, and received responses to their communications with NDR's Website from within California.

129. Plaintiffs and Class members did not consent for any of the Third Parties to read or learn the contents of their messages or communications or use or communicate the information obtained from the interception of their communications. Nor did Plaintiffs and Class members consent for NDR to aid, employ, or conspire with the Third Parties to permit or cause them to learn and/or use the information obtained from their use of NDR's Website.

130. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and Class members have been injured by the violations of Cal. Penal Code § 631 and each seek damages for the greater of $5,000 or three times the actual amount of damages, as well as injunctive relief.

COUNT II
Violation of CIPA
Cal. Penal Code 638
(Against Defendants Google and Claritas)

131. Plaintiffs repeat the allegations contained in the foregoing paragraphs 1 through 120 as if fully set forth herein.

132. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

133. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

134. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

135. The technologies designed by the Third Parties are "pen registers" because they are a "device or process" that "capture[d]" the "routing, addressing, or signaling information"—the IP address—from the electronic communications transmitted by Plaintiffs' and the Class's computers. Cal. Penal Code § 638.50(b).

136. At all relevant times, Defendant installed Google Analytics and Claritas on its Website to collect Plaintiffs' and Class Members' IP addresses.

137. Defendant did not obtain a court order to install or use the cookies.

138. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and Class Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class, respectfully request that this Court:

i. Enter an order certifying the proposed Class pursuant to Federal Rule of Civil Procedure 23;

ii. Enter an order appointing Plaintiffs as representatives of the Class;

iii. Enter an order appointing Plaintiffs' counsel as Class Counsel;

iv. Enter an order for injunctive and declaratory relief as described herein, including but not limited to:

a. Enjoining Defendant, its affiliates, associates, officers, employees and agents from transmitting or disclosing Plaintiffs' and the proposed Class members' PFI and the contents of their communications to unauthorized Third Parties;

b. Enjoining Defendant, its affiliates, associates, officers, employees and agents from taking Plaintiffs' and the Class members' PFI and the contents of their communications, and any other data except that for which appropriate notice and consent is provided;

v. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

vi. Enter judgment in favor of Plaintiffs and each of the other members of the Class for damages suffered as a result of Defendant's conduct alleged herein, including compensatory, statutory, and punitive damages; as well as equitable relief including restitution and disgorgement, to include interest and prejudgment interest;

vii. Award Plaintiffs and members of the Class pre- and post- judgment interest as provided by law;

viii. Award Plaintiffs their reasonable attorneys' fees and costs; and

ix. Grant such other and further legal and equitable relief as the court deems just and equitable.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: December 2, 2024

Respectfully submitted,

/s/ Samuel R. Jackson

Samuel R. Jackson (SBN 5332325)
Joseph Henry (Hank) Bates, III (*pro hac vice* forthcoming)
CARNEY BATES & PULLIAM, PLLC
One Allied Drive, Suite 1400
Little Rock, Arkansas 72202
Tel: (501) 312-8500
Fax: (501) 312-8505
Email: sjackson@cbplaw.com
Email: hbates@cbplaw.com

Attorneys for Plaintiffs